Sage
Application Service Provider Privacy & Security Policies

Access	A customer's access to Intergy On-Demand by Sage is through a standard web browser. Sage Software recommends the following: Internet Explorer 6.0 or higher and IE 7.0; a personal computer with a processor of 850 Mhz Pentium or equivalent with memory of 512 MB RAM minimum and Windows XP SP2 or higher; and an Internet connectivity speed of 512 kbps minimum or 62 kbps per user.
Authorization	Sage Software requires each Provider License and User to have a user name and password at two levels; a first level to access the hosted server and a second level to access the Intergy application. The first level access to the hosted server requires the user's names to be recorded at our datacenter and the second level access to the Intergy application is managed by a member of management at the practice. In addition, the Intergy application requires setup for each user to clarify what parts of the application the user may enter and use. Passwords are controlled by the customer.
Authentication	The subscription services employ encryption to reduce the probability of an unauthorized interception of information transmitted. Sage Software uses industry-standard encryption technology (e.g., 3.0 Secure Socket Layer protocol with 128-bit public key encryption technology) in arranging for the access to the hosted server and use of the software. It is the customer's responsibility not to access the hosted server or application from a location that is not secure or would violate applicable law or otherwise be inappropriate.
Audit	The hosted server is monitored 24/7 by Sage Software's world class datacenter. The datacenter is Vericenter, part of SunGard and has completed a successful SAS-70 Type II Audit. The datacenter employs best practices for providing a secure, stable datacenter environment. This includes multiple security measures to enhance physical security including security guards at each nondescript, unmarked building assist in physical access controls, badge-only access, man trap entry and/or biometric readers, as well as ongoing video surveillance.
Secondary Uses of Data	No, not at this time.
Data Ownership	The client owns the data, but not the hosted server or application.

*The information provided above is for informative purposes only. Sage Software Healthcare, Inc., reserves the right to amend any information contained herein.